Welcome to the PIA for FY 2010!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:
VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program. More information can be found by reading VA 6508.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: http://vaww.privacy.va.gov/PIA.asp

Roles and Responsibilities:
Roles and responsibilities for the specific process are clearly defined for all levels of staff in the Privacy Impact Assessment Handbook 6202.2 referenced in the procedure section of this document.

a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Handbook 6202.2.

b. Records Officer is responsible for supplying records retention and deletion schedules.

c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Handbook 6202.2 and to immediately report all anomalies to the Privacy Service and appropriate management chain.

d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.

e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

__Definition of PII (Personally Identifiable Information)__

Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect indentify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

__Macros Must Be Enabled on This Form__

To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at

(FY 2010) PIA: System Identification

Program or System Name:	Region I > VHA > VISN 18 >Amarillo VAHCS > Vista
OMB Unique System / Application / Program Identifier (AKA: UPID #):	Exhibit 300 ID: 029-00-01-11-01-1180-00

Description of System / Application / Program:

The Amarillo VA Health Care System uses ***VistA Legacy*** (formerly Decentralized Hospital Computer Program (DHCP), an integrated hospital information system. DHCP was an M-based internally developed portfolio and ***VistA Legacy*** encompasses DHCP and a variety of other clinical and administrative applications, some on single-use platforms.VA VISTA contains the AVAHCS patient database and the menu options which allow AVAHCS staff members access to the information contained within the patient database. VistA is currently running on a core platform, Virtual Memory System (VMS)/Cache.

Facility Name:	Amarillo VAHCS		
Title:	Name:	Phone:	Email:
Privacy Officer:	Bob Auffrey	806-355-9703 x	Robert.Auffrey@va.gov
Information Security Officer:	Steve Tyrer	806-355-9703 x7065	Steve.Tyrer@va.gov

Chief Information Officer:	Modesto Baca	806-355-9703 x4000	Modesto.Baca@va.gov
Person Completing Document:	Steve Tyrer	806-355-9703 x7065	Steve.Tyrer@va.gov
Second information Security Officer:	Deborah Heald	806-355-9703 x7190	Deborah.Heald@va.gov
System Owner:	Dr. James Laub	480-325-3131	James.Laub@va.gov
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	07/2009		
Date Approval To Operate Expires:	07/2011		
What specific legal authorities authorize this program or system:	Title 38, United States Code, section 7301(a).		
What is the expected number of individuals that will have their PII stored in this system:	125,000		
Identify what stage the System / Application / Program is at:	Operations/Maintenance		
The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.	16		
Is there an authorized change control process which documents any changes to existing applications or systems?	Yes		
If No, please explain:			
Has a PIA been completed within the last three years?	Yes		
Date of Report (MM/YYYY):	07/2010		

Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.

☑ Have any changes been made to the system since the last PIA?

□ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?

☑ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?

☑ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?

☑ Does this system/application/program collect, store or disseminate PII/PHI data?

☑ Does this system/application/program collect, store or disseminate the SSN?

If there is no Personally Identifiable Information on your system , please skip to TAB 12. (See Comment for Definition of PII)

(FY 2010) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? if the answer above is no, please skip to row 16.	Yes
For each applicable System(s) of Records, list:	
1. All System of Record Identifier(s) (number):	79VA19
2. Name of the System of Records:	VISTA-VA
3. Location where the specific applicable System of Records Notice may be accessed (include the URL):	http://www.rms.oit.va.gov/SOR_Records/79VA19.asp
Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?	Yes
Does the System of Records Notice require modification or updating?	No
	(Please Select Yes/No)
Is PII collected by paper methods?	Yes
Is PII collected by verbal methods?	Yes
Is PII collected by automated methods?	Yes
Is a Privacy notice provided?	Yes
Proximity and Timing: Is the privacy notice provided at the time of data collection?	Yes
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	Yes
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	Yes
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	Yes

(FY 2010) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	ALL	Health Care & Research, if approved	Verbal & Written	Verbal & Written
Family Relation (spouse, children, parents, grandparents, etc)	N/A			
Service Information	Paper	Health Care Benefits	Verbal & Written	Verbal & Written
Medical Information	Paper & Electronic	Medical Treatment	Verbal & Written	Verbal & Written
Criminal Record Information	Electronic/File Transfer	Medical Treatment	Verbal & Written	Verbal & Written
Guardian Information	N/A			
Education Information	Verbal		Verbal & Written	Verbal & Written
Benefit Information	Paper & Electronic	Health Care Benefits	Verbal & Written	Verbal & Written
Other (Explain)				

Data Type	Is Data Type Stored on your system?	**Source** (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Mandatory	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary	
Service Information	Yes	Veteran	Mandatory	
Medical Information	Yes	Veteran	Mandatory	
Criminal Record Information	Yes	Veteran	Mandatory	
Guardian Information	No		Mandatory	
Education Information	Yes	Veteran	Voluntary	
Benefit Information	Yes	Veteran	Mandatory	
Other (Explain)				
Other (Explain)				
Other (Explain)				

(FY 2010) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	Veterans Benefits	Yes	Medical Information Benefits Processing	Both PII & PHI	VA Directives and Handbooks
Other Veteran Organization					
Other Federal Government Agency					
State Government Agency					
Local Government Agency					
Research Entity					
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2010) PIA: Access to Records

Does the system gather information from another system?	No
Please enter the name of the system:	
Per responses in Tab 4, does the system gather information from an individual?	Yes
If information is gathered from an individual, is the information provided:	☑ Through a Written Request ☑ Submitted in Person ☑ Online via Electronic Form
Is there a contingency plan in place to process information when the system is down?	Yes

(FY 2010) PIA: Secondary Use

Will PII data be included with any secondary use request?	Yes
if yes, please check all that apply:	☑ Drug/Alcohol Counseling ☑ Mental Health ☑ HIV ☐ Research ☑ Sickle Cell ☐ Other (Please Explain)
Describe process for authorizing access to this data.	

Answer:	Written request from authorized source such as ROI request court order for records.

(FY 2010) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public? No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer: Data is collected by nationally mandated templates requiring specific sets of information requested. This insures standardization throughout the organization.

How is data checked for completeness?

Answer: Information entered into the system is check for completeness and accuracy via various checks and balances established throughout the system. Specific information can only be changed by certain personnel though use of person class, passwords, lease privilege, etc

What steps or procedures are taken to ensure the data remains current and not out of date?

Answer: Information is updated upon patient visit. Cliical reminders are also used to indicate info requires updating.

How is new data verified for relevance, authenticity and accuracy?

Answer: Information is stored in database and will automatically upload changed to various database applications. Data validation is performed through various audits which are performed by multiple sections and services.

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

(FY 2010) PIA: Retention & Disposal

What is the data retention period?

Answer: The data retention period is dependent upon the type of type contained in the record system. Personnel records, medical records, budget records, audit reports all have different NARA specified time frames that they must be kept for and then disposed of or archived off station. Paper medical records may be archived after complete scanning into the system, three years after death three years after the last visit. If not recalled from the archive the records will then be destroyed after 72 years.

Explain why the information is needed for the indicated retention period?

What are the procedures for eliminating data at the end of the retention period?

Answer: After the retention period has expired at the facility level, depending upon what the documents are, they may be shredded or they may be archived at a larger storage facility (as are medical records). If the full retention (75 years for medical records) has passes the documents will be disposed of using the current method in practice at the time.

Where are these procedures documented?

Answer: These procedures are fully documented within the Central Records Unit operating procedures and internally within the VISTA system

How are data retention procedures enforced?
Answer: Automatically enforced by the VISTA program.

Has the retention schedule been approved by the National Archives and Records Administration (NARA)
Yes

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)
Answer:

(FY 2010) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13? No
If Yes, How will parental or guardian approval be obtained?
Answer:

(FY 2010) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.

Yes

Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..

Yes

Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?

Yes

Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?

Yes

Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?

Yes

If 'No' to any of the 3 questions above, please describe why:
Answer:

Is adequate physical security in place to protect against unauthorized access?

Yes

If 'No' please describe why:
Answer:

Explain how the project meets IT security requirements and procedures required by federal law.
Answer: C&a completed 2008 and annual FISMA security control reviews.

Explain what security risks were identified in the security assessment? *(Check all that apply)*

☑ Air Conditioning Failure

□ Chemical/Biological Contamination

□ Blackmail

□ Bomb Threats

☑ Cold/Frost/Snow

☑ Communications Loss

☑ Computer Intrusion

☑ Data Destruction

☑ Data Disclosure

☑ Data Integrity Loss

☑ Denial of Service Attacks

□ Earthquakes

☑ Eavesdropping/Interception

☑ Fire (False Alarm, Major, and Minor)

☑ Flooding/Water Damage

☑ Hardware Failure

☑ Malicious Code

☑ Computer Misuse

☑ Power Loss

☑ Sabotage/Terrorism

☑ Storms/Hurricanes

□ Substance Abuse

☑ Theft of Assets

☑ Theft of Data

□ Vandalism/Rioting

☑ Errors (Configuration and Data Entry)

□ Burglary/Break In/Robbery

☑ Identity Theft

☑ Fraud/Embezzlement

Answer: (Other Risks)

Explain what security controls are being used to mitigate these risks. *(Check all that apply)*

☑ Risk Management

☑ Access Control

☑ Awareness and Training

☑ Contingency Planning

☑ Physical and Environmental Protection

☑ Personnel Security

☑ Certification and Accreditation Security Assessments

☑ Audit and Accountability

☑ Configuration Management

☑ Identification and Authentication

☑ Incident Response

☑ Media Protection

Answer: (Other Controls)

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

Answer: No changes were made.

<u>Availability Assessment:</u> If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☑ The potential impact is **<u>high</u>** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals. ☐ The potential impact is **<u>moderate</u>** if the loss of availability could be expected to have a serious adverse effect on operations, assets or ☐ The potential impact is **<u>low</u>** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
<u>Integrity Assessment:</u> If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☑ The potential impact is **<u>high</u>** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets ☐ The potential impact is **<u>moderate</u>** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals. ☐ The potential impact is **<u>low</u>** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
<u>Confidentiality Assessment:</u> If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization? **(Choose One)**	☑ The potential impact is **<u>high</u>** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets ☐ The potential impact is **<u>moderate</u>** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals. ☐ The potential impact is **<u>low</u>** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

The controls are being considered for the project based on the selections from the previous assessments? Yes

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

Please add additional controls:

(FY 2010) PIA: Additional Comments

Add any additional comments on this tab for any question in the form you want to comment on.
Please indicate the question you are responding to and then add your comments.

The amarillo VISTA system has been physically relocated to the Sacramento Regional Data Processing Center (RDPC). A read only backup database is available at the Amarillo site if the Primary site (Sacramento) and Secondary site (Denver) are both unavailable.

(FY 2010) PIA: VBA Minor Applications

Explain what minor application that are associated with your installation? *(Check all that apply)*

- Records Locator System
- Veterans Assistance Discharge System (VADS)
- LGY Processing
- Loan Service and Claims
- LGY Home Loans
- Search Participant Profile (SPP)
- Control of Veterans Records (COVERS)
- SHARE
- Modern Awards Process Development (MAP-D)
- Rating Board Automation 2000 (RBA2000)
- State of Case/Supplemental (SOC/SSOC)
- Awards
- Financial and Accounting System (FAS)
- Eligibility Verification Report (EVR)
- Automated Medical Information System (AMIS)290
- Web Automated Reference Material System (WARMS)
- Automated Standardized Performace Elements Nationwide (ASPEN)
- Inquiry Routing Information System (IRIS)
- National Silent Monitoring (NSM)
- Web Service Medical Records (WebSMR)
- Systematic Technical Accuracy Review (STAR)
- Fiduciary STAR Case Review
- Veterans Exam Request Info System (VERIS)
- Web Automated Folder Processing System (WAFPS)
- Courseware Delivery System (CDS)
- Electronic Performance Support System (EPSS)
- Veterans Service Representative (VSR) Advisor
- Loan Guaranty Training Website
- C&P Training Website

- Education Training Website
- VR&E Training Website
- VA Reserve Educational Assistance Program
- Web Automated Verification of Enrollment
- Right Now Web
- VA Online Certification of Enrollment (VA-ONCE
- Automated Folder Processing System (AFPS)
- Personal Computer Generated Letters (PCGL)
- Personnel Information Exchange System (PIES)
- Rating Board Automation 2000 (RBA2000)
- SHARE
- State Benefits Reference System
- Training and Performance Support System (TPSS)
- Veterans Appeals Control and Locator System (VACOLS)
- Veterans On-Line Applications (VONAPP)
- Automated Medical Information Exchange II (AIME II)
- Committee on Waivers and Compromises (COWC)
- Common Security User Manager (CSUM)
- Compensation and Pension (C&P) Record Interchange (CAPRI)
- Control of Veterans Records (COVERS)
- Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
- Fiduciary Beneficiary System (FBS)
- Hearing Officer Letters and Reports System (HOLAR)
- Inforce
- Awards
- Actuarial
- Insurance Self Service
- Insurance Unclaimed Liabilities
- Insurance Online

- Appraisal System
- Web Electronic Lender Identification
- CONDO PUD Builder
- Centralized Property Tracking System
- Electronic Appraisal System
- Web LGY
- Access Manager
- SAHSHA
- VBA Data Warehouse
- Distribution of Operational Resources (DOOR)
- Enterprise Wireless Messaging System (Blackberry)
- VBA Enterprise Messaging System
- LGY Centralized Fax System
- Review of Quality (ROQ)
- Automated Sales Reporting (ASR)
- Electronic Card System (ECS)
- Electronic Payroll Deduction (EPD)
- Financial Management Information System (FMI)
- Purchase Order Management System (POMS)
- Veterans Canteen Web
- Inventory Management System (IMS)
- Synquest
- RAI/MDS
- ASSISTS
- MUSE
- Bbraun (CP Hemo)
- VIC
- BCMA Contingency Machines
- Script Pro

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Minor app #1

Name

Description

Comments

□ Is PII collected by this min or application?

□ Does this minor application store PII?

If yes, where?

Who has access to this data?

Minor app #2

Name

Description

Comments

□ Is PII collected by this min or application?

□ Does this minor application store PII?

If yes, where?

Who has access to this data?

Minor app #3

Name

Description

Comments

□ Is PII collected by this min or application?

□ Does this minor application store PII?

If yes, where?

Who has access to this data?

Baker System

Dental Records Manager

Sidexis

Priv Plus

Mental Health Asisstant

Telecare Record Manager

Omnicell

Powerscribe Dictation System

EndoSoft

Compensation and Pension (C&P)

Montgomery GI Bill

Vocational Rehabilitation & Employment (VR&E) CH 31

Post Vietnam Era educational Program (VEAP) CH 32

Spinal Bifida Program Ch 18

C&P Payment System

Survivors and Dependents Education Assistance CH 35

Reinstatement Entitelment Program for Survivors (REAPS)

Educational Assistance for Members of the Selected Reserve Program CH 1606

Reserve Educational Assistance Program CH 1607

Compensation & Pension Training Website

Web-Enabled Approval Management System (WEAMS)

FOCAS

Work Study Management System (WSMS)

Benefits Delivery Network (BDN)

Personnel and Accounting Integrated Data and Fee Basis (PAID)

Personnel Information Exchange System (PIES)

Rating Board Automation 2000 (RBA2000)

SHARE

Service Member Records Tracking System

Veterans Assistance Discharge System (VADS)

VBA Training Academy

Veterans Service Network (VETSNET)

Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)

BIRLS

Centralized Accounts Receivable System (CARS)

Compensation & Pension (C&P)

Corporate Database

Control of Veterans Records (COVERS)

Data Warehouse

INS - BIRLS

Mobilization

Master Veterans Record (MVR

BDN Payment History

Explain what minor application that are associated with your installation? *(Check all that apply)*

X	ACCOUNTS RECEIVABLE	X	DRUG ACCOUNTABILITY	X	INPATIENT MEDICATIONS	X
X	ADP PLANNING (PLANMAN)	X	DSS EXTRACTS	X	INTAKE/OUTPUT	X
X	ADVERSE REACTION TRACKING	X	EDUCATION TRACKING	X	INTEGRATED BILLING	X
X	ASISTS	X	EEO COMPLAINT TRACKING	X	INTEGRATED PATIENT FUNDS	X
X	AUTHORIZATION/SUBSCRIPTION	X	ELECTRONIC SIGNATURE	X	INTERIM MANAGEMENT SUPPORT	X
X	AUTO REPLENISHMENT/WARD STOCK	X	ENGINEERING	X	KERNEL	X
X	AUTOMATED INFO COLLECTION SYS	X	ENROLLMENT APPLICATION SYSTEM	X	KIDS	X
X	AUTOMATED LAB INSTRUMENTS	X	EQUIPMENT/TURN-IN REQUEST	X	LAB SERVICE	X
X	AUTOMATED MED INFO EXCHANGE	X	EVENT CAPTURE	X	LETTERMAN	X
X	BAR CODE MED ADMIN	X	EVENT DRIVEN REPORTING	X	LEXICON UTILITY	X
X	BED CONTROL	X	EXTENSIBLE EDITOR	X	LIBRARY	X
X	BENEFICIARY TRAVEL	X	EXTERNAL PEER REVIEW	X	LIST MANAGER	x
X	CAPACITY MANAGEMENT - RUM	X	FEE BASIS	X	MAILMAN	X
X	CAPRI	X	FUNCTIONAL INDEPENDENCE	X	MASTER PATIENT INDEX VISTA	
X	CAPACITY MANAGEMENT TOOLS	X	GEN. MED. REC. - GENERATOR	X	MCCR NATIONAL DATABASE	X
X	CARE MANAGEMENT	X	GEN. MED. REC. - I/O	X	MEDICINE	X
X	CLINICAL CASE REGISTRIES	X	GEN. MED. REC. - VITALS	X	MENTAL HEALTH	X
X	CLINICAL INFO RESOURCE NETWORK	X	GENERIC CODE SHEET	X	MICOM	X
X	CLINICAL MONITORING SYSTEM	X	GRECC	X	MINIMAL PATIENT DATASET	X
X	CLINICAL PROCEDURES	X	HEALTH DATA & INFORMATICS	X	MYHEALTHEVET	X
X	CLINICAL REMINDERS	X	HEALTH LEVEL SEVEN	X	Missing Patient Reg (Original) A4EL	X
X	CMOP	X	HEALTH SUMMARY	x	NATIONAL DRUG FILE	X
X	CONSULT/REQUEST TRACKING	X	HINQ	X	NATIONAL LABORATORY TEST	X
X	CONTROLLED SUBSTANCES	X	HOSPITAL BASED HOME CARE	X	NDBI	X
X	CPT/HCPCS CODES	X	ICR - IMMUNOLOGY CASE REGISTRY	X	NETWORK HEALTH EXCHANGE	X
X	CREDENTIALS TRACKING	X	IFCAP	X	NOIS	X
X	DENTAL	X	IMAGING	X	NURSING SERVICE	
X	DIETETICS	X	INCIDENT REPORTING	X	OCCURRENCE SCREEN	X
X	DISCHARGE SUMMARY	X	INCOME VERIFICATION MATCH	X	ONCOLOGY	X
X	DRG GROUPER		INCOMPLETE RECORDS TRACKING	X	ORDER ENTRY/RESULTS REPORTING	X

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Minor app #1

Name		Description	Comments

□ Is PII collected by this min or application?

□ Does this minor application store PII?

If yes, where?

Who has access to this data?

Minor app #2

Name		Description	Comments

□ Is PII collected by this min or application?

Does this minor application store PII?

□ If yes, where?

Who has access to this data?

Minor app #3

Name		Description	Comments

□ Is PII collected by this min or application?

Does this minor application store PII?

□ If yes, where?

Who has access to this data?

OUTPATIENT PHARMACY	X	SOCIAL WORK
PAID		SPINAL CORD DYSFUNCTION
PATCH MODULE	X	SURGERY
PATIENT DATA EXCHANGE	X	SURVEY GENERATOR
PATIENT FEEDBACK	X	TEXT INTEGRATION UTILITIES
PATIENT REPRESENTATIVE	X	TOOLKIT
PCE PATIENT CARE ENCOUNTER	X	UNWINDER
PCE PATIENT/IHS SUBSET	X	UTILIZATION MANAGEMENT ROLLUP
PHARMACY BENEFITS MANAGEMENT	X	UTILIZATION REVIEW
PHARMACY DATA MANAGEMENT	X	VA CERTIFIED COMPONENTS - DSSI
PHARMACY NATIONAL DATABASE	X	VA FILEMAN
PHARMACY PRESCRIPTION PRACTICE	X	VBECS
POLICE & SECURITY	X	VDEF
PROBLEM LIST	X	VENDOR - DOCUMENT STORAGE SYS
PROGRESS NOTES	X	VHS&RA ADP TRACKING SYSTEM
PROSTHETICS	X	VISIT TRACKING
QUALITY ASSURANCE INTEGRATION	X	VISTALINK
QUALITY IMPROVEMENT CHECKLIST	X	VISTALINK SECURITY
QUASAR	X	VISUAL IMPAIRMENT SERVICE TEAM ANRV
RADIOLOGY/NUCLEAR MEDICINE	X	VOLUNTARY TIMEKEEPING
RECORD TRACKING	X	VOLUNTARY TIMEKEEPING NATIONAL
REGISTRATION	X	WOMEN'S HEALTH
RELEASE OF INFORMATION - DSSI	X	CARE TRACKER
REMOTE ORDER/ENTRY SYSTEM		
RPC BROKER		
RUN TIME LIBRARY		
SAGG		
SCHEDULING		
SECURITY SUITE UTILITY PACK		
SHIFT CHANGE HANDOFF TOOL		

(FY 2010) PIA: Minor Applications

Add any information concerning minor applications that may be associated with your system. Please indicate the name of the minor application, a brief description, and any comments you may wish to include. If you have more than 3 minor applications please copy then below sections as many times as needed.

Minor app #1

Name	Description	Comments

Is PII collected by this min or application?

Does this minor application store PII?

If yes, where?

Who has access to this data?

Minor app #2

Name	Description	Comments

Is PII collected by this min or application?

Does this minor application store PII?

If yes, where?

Who has access to this data?

Minor app #3

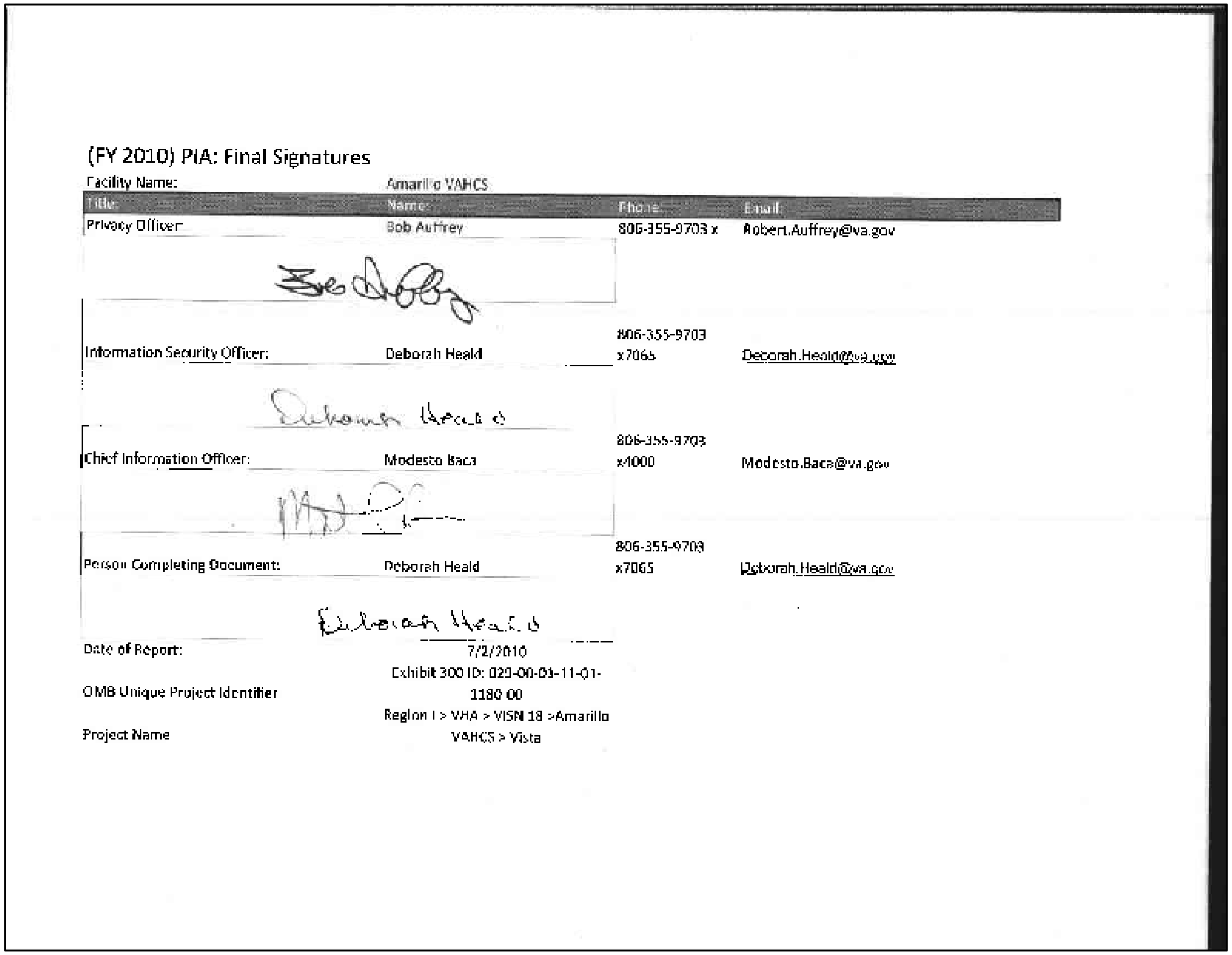
Name	Description	Comments

Is PII collected by this min or application?

Does this minor application store PII?

If yes, where?

Who has access to this data?



(FY 2010) PIA: Final Signatures

Facility Name:	Amarillo VAHCS		
Title:	Name:	Phone:	Email:
Privacy Officer:	Bob Auffrey	806-355-9703 x	Robert.Auffrey@va.gov
Information Security Officer:	Deborah Heald	806-355-9703 x7065	Deborah.Heald@va.gov
	Deborah Heald		
Chief Information Officer:	Modesto Baca	806-355-9703 x4000	Modesto.Baca@va.gov
Person Completing Document:	Deborah Heald	806-355-9703 x7065	Deborah.Heald@va.gov
	Deborah Heald		
Date of Report:	7/2/2010		
OMB Unique Project Identifier	Exhibit 300 ID: 029-00-01-11-01-1180 00		
Project Name	Region I > VHA > VISN 18 >Amarillo VAHCS > Vista		